ABSTRACT OF THE DISCLOSURE

A key management of cryptographic keys has a data package including one or more cryptographic keys that are transferred to a personal device 100 from a secure processing point 150 of a device assembly line in order to store device specific cryptographic keys in the personal device 100. In response to the transferred data package, a backup data package is received by the secure processing point 150 from the personal device 100, which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage 125 of a chip 110 included in the personal device 100. The secure processing point 150 is arranged to store the backup data package, together with an associated unique chip identifier read from the personal device 100, in a permanent, public database 170.

Fig. 1